REMARKS

Claims 1-33 remain in this application. **Claim 34 has been added**. No claims have been canceled or amended.

CLAIM REJECTIONS – 35 U.S.C. § 102

The Office Action rejected Claims 1-6, 12-17, and 23-28 under 35 U.S.C. § 102(e) as allegedly unpatentable over Jalili, U.S. Patent No. 6,209,104 ("Jalili"). The rejection is respectfully traversed.

Independent Claim 1 recites a method for verifying the legitimacy of an untrusted mechanism. The method comprises:

> submitting **a first set of information and a second set of information** to an untrusted mechanism in a **sequence** that is unpredictable to the untrusted mechanism;
> receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information;
> determining whether each response received from the untrusted mechanism is a correct response; and
> in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate.

The method of Claim 1 is quite advantageous because it provides an effective means for testing the legitimacy of any untrusted mechanism. According to the method, an untrusted mechanism is determined to not be legitimate if any of the untrusted mechanism's responses to a sequence of information set submissions is an incorrect response. Because the sequence in which information sets are submitted to an untrusted mechanism is unpredictable to the untrusted mechanism, it is highly difficult, if not impossible, for an illegitimate untrusted mechanism to "fake" correct responses to all of the submissions.

Jalili does not teach or suggest such a method. Instead, Jalili discloses a technique whereby information that identifies a password can be transmitted over a network without transmitting the actual password over the network, thereby preventing malicious parties from intercepting and using the password. More specifically, Jalili discloses that a server generates an image that contains randomly arranged icons. Each icon represents a different number or letter. The server stores position correlation information that correlates the position of each icon with the number or letter that the icon represents. The server sends the image—but not the position correlation information—to a client, which displays the image to a user. The user selects icons from the image, in the same way that the user would select numbers and letters from a keyboard or keypad, to input the user's password. However, instead of transmitting the actual password to the server over the network, the client transmits only the positions of the icons that the user selected. The server receives the positions and uses the position correlation information to determine the numbers or letters to which the positions correspond, thereby constructing the actual password at the server. The server then determines whether the password is correct. A malicious party that intercepts the positions transmitted over the network cannot derive the password from the positions because the malicious party does not possess the position correlation information.

The Office Action analogizes the first and second sets of information recited in Claim 1 to a first set of icons that represent numbers/letters that **are** in the password and a second set of icons that represent numbers/letters that **are not** in the password, respectively, that are allegedly disclosed by Jalili. Nowhere in Jalili are the icons expressly grouped into such sets; the reasoning behind the Office Action seems to be that, because some of the icons **supposedly must** represent letters/numbers that **are** in the password and some of the icons **supposedly must** represent letters/numbers that **are not** in the password, the sets are inherently disclosed as a result of the express disclosure of an image that contains such icons (the latter supposition is demonstrated below to be fallacious). The Office Action apparently reasons that, because Jalili's server receives each user-selected icon's position from a client, the server receives a "response" for each "submission" in the first set, at least in a scenario in which the user selects only those icons that represent numbers/letters that are in the password. The Office Action also apparently reasons that, because Jalili's server determines whether the numbers/letters represented by the user-selected icons result in the correct password, the server determines whether each "response" is a "correct response." Additionally, the Office Action apparently reasons that, because Jalili's server does not allow access to a client that gets at least one number/letter of the password wrong, the server determines the client to be illegitimate if any "response" is not a "correct response."

Claim 1 recites submitting a **sequence** to an untrusted mechanism. The Office Action analogizes the sequence recited in Claim 1 to the **image** disclosed in Jalili. However, an "image" is not a "sequence." A sequence is characterized by an inherent first-to-last ordering. For example, in the numeric sequence "12345," the number "1" inherently occurs first in the sequence, while the number "5" inherently occurs last in the sequence. There is no such inherent first-to-last ordering in an image. Although a particular icon in an image is spatially related to other icons in the image by virtue of being above, below, left of, or right of the other icons, there is no inherent notion of first-to-last ordering in a two-dimensional image. Because an image lacks inherent first-to-last ordering, an image is significantly different from a sequence. At least because Jalili fails to disclose the **sequence** recited in Claim 1, Jalili fails to anticipate Claim 1 under 35 U.S.C. §102(e), and Claim 1 is patentable over Jalili.

Additionally, Jalili fails to teach or suggest the **first and second sets of information** that are recited in Claim 1. As is discussed above, Jalili does not expressly disclose the two sets of icons—one set allegedly comprising icons that represent numbers/letters that are in the password and one set allegedly comprising icons that represent numbers/letters that are not in the password—that form the entire basis of the Office Action's apparent reasoning; the Office Action merely assumes that such separate sets necessarily exist. In actuality, two such sets do not necessarily exist. Even taking into consideration all of Jalili's teachings, it still could be the case that the **only** icons contained in the server-generated image are icons that represent number/letters that are in the password. An example below demonstrates the truth of this assertion.

Suppose that the password is a 4-digit PIN. It is entirely possible that every legitimate PIN used by a system is some combination of 4 numbers from the set (1,2,3,4). In such a system that adopted Jalili's technique, it would only be necessary to display 4 icons; one representing the number "1," one representing the number "2," one representing the number "3," and one representing the number "4." There could exist many different PINs that contained **all** of these numbers (e.g., "1234," "2341," "3412," etc.). In such a system, the **order** of the numbers in the PIN, in addition to the **inclusion** of the numbers in the PIN, matters. It might be the case that every user's PIN contains all four numbers. Indeed, there is no requirement in Jalili that each user's PIN must be unique.

This example clearly shows that it **does not necessarily follow** from Jalili's disclosure that the server generates an image that contains at least some icons that represent numbers/letters that are not in a password. It is consistent with Jalili's disclosure to assume that the server might always generate an image that **only** contains icons that represent letters/numbers that are in the password. **Jalili does not teach or suggest the notion that the image must contain a set of icons that represent letters/numbers that are not in the password**. Such a notion is the product of assumptions that Jalili does not sustain.

Thus, Jalili fails to teach or suggest the first and second information sets that are recited in Claim 1. For at least this reason, Jalili fails to anticipate Claim 1 under 35 U.S.C. §102(e), and Claim 1 is patentable over Jalili.

Applicants further submit that Claims 2-6, which depend from Claim 1 and which recite further advantageous aspects of the invention, are also patentable over Jalili for at least the reasons given above in connection with Claim 1.

Claims 12-17 are apparatus claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 12-17 are patentable over Jalili for at least the reasons given above in connection with Claims 1-6, respectively.

Claims 23-28 are computer-readable medium claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 23-28 are patentable over Jalili for at least the reasons given above in connection with Claims 1-6, respectively.

CLAIM REJECTIONS – 35 U.S.C. § 103

The Office Action rejected Claims 7-11, 18-22, and 29-33 under 35 U.S.C. § 103 as allegedly unpatentable over Jalili in view of Shostack et al., U.S. Patent No. 6,298,445 B1 ("Shostack"). The rejection is respectfully traversed.

Independent Claim 7 recites a method for verifying the legitimacy of an untrusted signature verification mechanism. The method comprises:

> submitting **a first signature and a second signature** to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and **said second signature being known to be unverifiable**;
> receiving a response from the untrusted mechanism for each submission of either said first signature or said second signature;
> determining whether each response received from the untrusted mechanism is a correct response; and
> in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate.

The method of Claim 7 provides an effective means for testing the legitimacy of an untrusted signature verification mechanism.

Jalili does not teach or suggest such a method. Jalili is discussed above with reference to Claim 1. As is discussed above, Jalili fails to teach or suggest two sets of information. In rejecting Claim 7, the Office Action merely analogizes the "second signature," which is "known to be unverifiable," to the alleged set of Jalili's icons that represent letters/numbers that that are not contained in the password. As is discussed above with reference to Claim 1, though, Jalili does not actually teach or suggest such a set. Just as Jalili fails to teach or suggest two separate sets, Jalili also fails to teach or suggest two separate signatures, one being known to be unverifiable.

Shostack also fails to teach or suggest two separate signatures, one being known to be unverifiable. In fact, the Office Action does not even allege that Shostack teaches or suggests this feature. The Office Action relies upon Shostack only to disclose, allegedly, the use of digital signatures to authenticate the integrity of a software enhancement.

Eveh combined (assuming arguendo that it would have been obvious to combine the references), Jalili and Shostack fail to teach or suggest a first signature and a second signature, the second signature being known to be unverifiable. Thus, even if the references were combined, they would still fail to disclose or suggest this aspect of Claim 7. For at least these reasons, Claim 7 is patentable over Jalili and Shostack, taken individually or in combination.

Claims 8-11, which depend from Claim 7 and which recite further advantageous aspects of the invention, are also patentable over Jalili and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claim 7.

Claims 18-22 are apparatus claims, which are analogous to the methods of Claims 7-11, respectively. Claims 18-22 are patentable over Jalili and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claims 7-11, respectively.

Claims 29-33 are computer-readable medium claims, which are analogous to the methods of Claims 7-11, respectively. Claims 29-33 are patentable over Jalili and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claims 7-11, respectively.

For at least the reasons set forth above, Applicants respectfully submit that all pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all pending claims is respectfully solicited.

The Examiner is invited to telephone the undersigned at (408) 414-1080 to discuss any issue that may advance prosecution.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: September 8, 2004

Christian A. Nicholes
Reg. No. 50,266

1600 Willow Street
San Jose, California 95125-5106
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on September 8, 2004 by